Multimedia Tools and Applications (2024) 83:3895–3916
https://doi.org/10.1007/s11042-023-15554-z

Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking

Tanya Koohpayeh Araghi[1,2] · David Megías[1,2]

Received: 3 June 2022 / Revised: 16 February 2023 / Accepted: 18 April 2023 /
Published online: 20 May 2023

Abstract

In this paper, an analysis on hybrid Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for image watermarking is carried out to investigate the effect of a deeper level of the SVD on imperceptibility and robustness to resist common signal processing and geometric attacks. For this purpose, we have designed two hybrid watermarking schemes, the first one with DWT and first level of SVD, whereas, in the second scheme, the same design is employed with a second level of SVD. In this experiment, a comprehensive analysis is performed on the two designed schemes and the effect of robustness and imperceptibility is compared in the first and second levels of SVD in each DWT sub-band. Having analyzed more than 100 medical and non-medical images in standard datasets and real medical samples of patients, the experimental outcomes show a remarkable increase in both imperceptibility and robustness in the second level of SVD, in comparison to the first level. In addition, the achieved result shows that the SVD2 scheme offers the highest imperceptibility in the LL sub-band (more than 60 dB on average PSNR), with satisfactory robustness against noise attacks, but less persistence in some geometric attacks such as cropping. For the HH sub-band, strong robustness against all types of tested of attacks is obtained, though its imperceptibility is slightly lower than the achieved PSNR in the LL sub-band. In HH sub-band, an average growth of 5 dB in PSNR and 2% in NC can be observed from the second level of SVD in comparison to the first level. These results make SVD2 a good candidate for content protection, especially for medical images.

Keywords Hybrid image watermarking · DWT · SVD1 · SVD2 · Security · Robustness · Imperceptibility

✉ Tanya Koohpayeh Araghi
tkoohpayeharaghi@uoc.edu

[1] Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Barcelona, Spain

[2] CYBERCAT-Center for Cybersecurity Research of Catalunya, Barcelona, Spain

1 Introduction

Nowadays, the necessity of copyright protection in digital media has led to a massive growth in the field of digital watermarking, where researchers are motivated to devise innovative solutions for ownership protection [7, 38].

However, facing signal processing manipulations are inevitable, because of the influence of noise and destructive signals from the communication channels and the medical devices. Particular care must be taken to ensure the robustness of the embedded watermark against such attacks to attain the required functionalities in the target applications [15, 50].

For medical images, regarding applications such as tele-radiography, in which these images are being transferred on electronic networks, the watermarked images must be robust against the noise stemming from the transmission channel [8].

Digital image watermarking is defined as embedding secret symbols (known as watermark) into the digital media for copyright protection and authentication verification [9, 20, 42, 43]. The watermark should be imperceptible, so that the end user cannot perceive any visual effect from the watermarked image. Although the watermark image is not supposed to degrade the quality of the content, a little degradation is acceptable in some applications in order to achieve high robustness or low cost [3, 17, 27].

The watermarked image should be robust meaning that it should be impossible to remove without serious damage to the image itself, and it should resist a wide range of attacks [12]. In addition, the watermark must not be recovered or even altered without a secret key [37]. In designing a watermarking scheme, four essential properties, namely imperceptibility, robustness, capacity and security, should be taken into consideration. However, according to the application, some of these properties can be more prioritized [7, 24, 32].

Considering all the above issues, we designed and implemented two hybrid Discrete Wavelet Transform and Singular Value Decomposition (DWT + SVD) schemes in the first and second levels of SVD in order to investigate the performance of each scheme.

The second level of SVD is a novel idea which was proposed for the first time in our previous work [14]. But, So far, a full investigation and analysis to show the performance of this technique in comparison to traditional SVD, has not been performed especially when this technique is combined with DWT. The importance of this comparison and analysis stems from the need of designing high performance watermarking schemes with less computational complexity and maximum imperceptibility and robustness. In this paper, we investigate the effect of a deeper level of SVD on the performance of hybrid DWT + SVD schemes and present the results of this comparison to employ high quality watermarking in order to reduce the computational burden and save resources, with minimum use of auxiliary techniques, such as artificial intelligence, genetic algorithm, or any other technique.

For this purpose, we have designed and implemented the two proposed schemes under the same processor, CPU speed, memory and similar methodologies with identical cover and watermark images. Moreover, this comparison is analyzed for all four DWT sub- bands in both types of medical and typical images. Then, the robustness of both schemes are tested by applying 11 most prevalent attacks including geometric and signal processing attacks to show the effectiveness of a deeper level of SVD in image watermarking for content and copyright protection.

The rest of the paper is organized as follows. In Section 2, we mentioned some state of the art techniques using DWT and SVD. In Section 3, theoretical background and essential definitions related to the proposed schemes are described. Section 4 defines the methodology that has been employed for the two SVD 1 and SVD 2 schemes. In Section 5, the experimental results and an inclusive assessment for both schemes are presented. Section 6 analyzes and evaluates both schemes in comparison with several other hybrid DWT and one level SVD schemes, and discusses the results. Finally, Section 7 presents the conclusions and future work.

2 Literature review

Today duo to easy use of the ubiquitous media such as mobile phones or through the social media many people transfer various types of data such as video, audio and images or text to circulate news over the Internet. This data can be manipulated with no trouble using a number of accessible software. Steganography and watermarking are two important approaches to provide hidden communication [23]. Some researchers proved data authentication and integrity using steganography [18, 19, 35, 36]. However, in this research our focus is on the watermarking techniques.

The classification of digital watermarking schemes can be carried out in various ways. One of them is based on the domain in which the watermark is embedded. In terms of domain, image watermarking schemes can be classified as either spatial or transformed domain. The simplicity in implementation and low cost of the operations are two important properties of the spatial domain techniques, but the drawback of this approach is low robustness against signal processing and geometric attacks. Instead, transformed domain techniques are usually employed for robust watermarking to ensure resistance of the watermarked image against the mentioned attacks [13, 39, 40]. Several examples of transformed domain techniques are the Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). Later on, the DWT and the SVD techniques that are used for the proposed schemes are discussed in detail.

Amongst these techniques an optimum resistance against attacks has been achieved by hybrid DWT and SVD techniques [16, 28, 29, 34, 48]. Hence, we focus on the combination of these two techniques in the literature review. Ahmadi et al. [2] proposed a blind dual watermarking scheme for the purpose of copyright protection as well as image authentication. The authors embedded two types of fragile and robust watermark in color images. In order to achieve an optimum balance between imperceptibility and robustness they used particle swarm optimization (PSO) technique. The importance of this research is on preserving both image integrity and robustness which proves the novelty of the author's idea that can be appropriate for some applications such as fake news detection. However, the resistance of the scheme against image compression needs to be enhanced.

Zeng et al. [51], proposed a hybrid watermarking scheme using Non-sub sampled Contourlet Transformation (NSCT), to find low frequency sub-bands. The authors used DWT in the second level in the low frequency sub-band stemming from the previous step and performed SVD on each block of low frequency sub-band of DWT. This scheme shows a good balance between imperceptibility and robustness. However, the capacity of the scheme needs to be improved.

Wang and Zhao [49], proposed a scheme using a global optimization algorithm named Wang–Landau (WL) sampling to find the best embedding coefficients to hide information on three level DWT and SVD transform. Experimental results prove the appropriateness of the scheme against attacks with a high PSNR. Nonetheless, the robustness for histogram equalization, gamma correction and rotation attacks needs to be improved.

Aree et al. [34] proposed an enhanced zigzag technique for improving imperceptibility using HL and HH sub-bands of 2 level DWT decomposition and SVD transform. The scheme shows better efficiency than typical zigzag techniques, but it needs to be enhanced in terms of reducing the computational time and cost.

All mentioned schemes used additional techniques to make a balance between imperceptibility and robustness, which impose a burden on the computational cost and complexity of the algorithm. Using 2 levels of SVD can compensate for the additional techniques to achieve an optimum balance between imperceptibility and robustness. In the following the theoretical background is explained in order for better understanding of the proposed schemes.

3 Theoretical background

In this section we briefly explain the fundamental techniques used in designing the proposed schemes namely Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD). The calculation of the second level of SVD is described in Section 4 (methodology).

3.1 Discrete wavelet transform (DWT)

Wavelet transform is known as a fundamental tool in watermarking and image processing applications due to its remarkable energy compaction properties [4, 25, 44, 48]. DWT is a multipurpose mathematical transform which splits an image into four frequency sub-bands based on small waves with varying frequencies and limited periods. For each level of decomposition in DWT, a lower resolution of approximation component (LL) and three other corresponding detail components like horizontal (HL), vertical (LH) and diagonal (HH) are represented [1, 21, 22, 45].

By transforming an image using wavelets, most of the information will be located in the LL sub-band. Therefore, this sub-band is known as the approximate image. The other sub-bands include some details like the edges and textures of the original image. For example, LH keeps the majority of the vertical features of the image related to the horizontal edges, whereas HL contains horizontal detail of information corresponding to the vertical edges. The LL sub-band can be decomposed again into further levels of decompositions until the ideal required level by the application is achieved [10, 26].

A watermark can be any information represented with a sequence of bits to be embedded in the host or cover image. In different works, the watermark itself is another image, e.g. a logotype usually smaller or at the same size of the cover. In such case, it is referred as the watermark image. The watermark image can be embedded in every frequency sub-band of the DWT as a low-power noise enjoying the multi resolution technique. If it is embedded into the high frequency sub-bands, it will affect the imperceptibility of the watermark, because the values of the coefficients in the HH sub-band are typically small. On the other hand, low frequency sub-bands contain higher values that make it possible to embed the

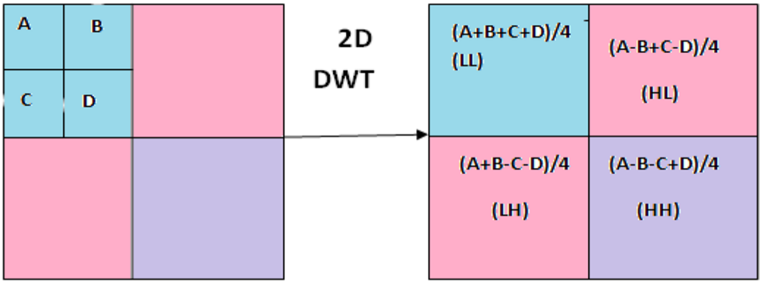


Fig. 1 New values of an image after Haar DWT decomposition

watermark bits (or pixels) more imperceptibly. Figure 1 represents the values of an image in each frequency sub-band after one level Haar wavelet decomposition.

3.2 Singular value decomposition (SVD)

SVD is defined based on the theorem of linear algebra confirming that a rectangular matrix A can be decomposed into three matrices, an orthogonal matrix U, a diagonal matrix S and the transpose of an orthogonal matrix V. In other words, a digital image can be shown as nonnegative scalar elements of a matrix. Let A be a rectangular m × n matrix (m ≥ n), then according to SVD, the decomposition can be written as follows:

$$A = USV^T, \tag{1}$$

where $UU^T = I_m$ and $VV^T = I_{mn}$,$VV^T = I_{nm}$, the columns of U are orthonormal eigenvectors of AA^T, the columns of V are orthonormal eigenvectors of A^TA, and S is a diagonal matrix including the square roots of the eigenvalues of U or V in descending order. In case of having r ($r \leq n$) as the rank of the matrix A, the elements of the diagonal matrix S are shown based on Expression (2) and the matrix A is represented as in Expression (3):

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r \geq \sigma_{r+1} = \sigma_{r+2} \cdots = \sigma_n = 0, \tag{2}$$

$$A = \sum_{k=1}^{r} \sigma_k u_k v_k^T, \tag{3}$$

where u_k and v_k are the k-th eigenvectors of U and V respectively, and σ_k is the k-th singular value [5, 30].

There are some benefits in using singular value decomposition in digital image watermarking. The first one is the lack of requiring a fixed size memory; since it can be represented by a rectangle or a square. Secondly, the SVD transform improves the precision and reduces the memory restriction. Thirdly, in case of embedding a watermark image, the singular values of the host image are affected to a lower extent.

The larger singular values preserve most of the energy of an image as well as resisting against signal processing and geometric attacks. The singular values represent the luminance of an image layer whilst the succeeding pair of singular vectors represents the geometry of the image layer [28, 33, 46].

4 Methodology

In SVD decomposition, the largest singular values carry most of the energy of the image; hence, embedding a watermark into these coefficients results in a robust watermarked image. Inspired by this idea, we have designed and implemented our hybrid watermarking schemes, one, a hybrid scheme in the second level of SVD, and another with only one level of SVD, to investigate the robustness and the imperceptibility of the watermarked images for both schemes. In one scheme, the host image is transformed using DWT and one level of SVD to embed the watermark image in the singular values of the host image using all four DWT sub-bands. The other scheme uses two levels of SVD in such a way that, firstly, the host image is decomposed by DWT and each sub-band of it, is divided into non-overlapping n × n matrices, then SVD is applied on each n × n blocks to collect all largest singular values located in S (1, 1) of each block in a separate matrix in order to hide the watermark in the singular values of this matrix, after applying the second level of SVD. We denote "SVD2" as the use of a second level of SVD, whereas "SVD1" refers to a single level of the SVD.

The feasibility of implementing SVD2 is tested and verified in [29] , and the value of n for image blocking is selected as 16, whereas the reason of this selection is provided in [11]. Finally, a pre-processing step is performed on the watermark image in both schemes in order to repeat the watermark redundantly, so that the sizes of both watermark and host images become equal. In the sequel, the details of embedding and extraction of each scheme are discussed.

Our effort is to analyze the efficiency of SVD1 and SVD2. Therefore, these two schemes are designed and implemented based on approximate matching algorithms, such as watermark preparation and embedding, with the same resources like memory and CPU speed. The embedding and extraction flowcharts for both schemes are shown in Figs. 2 and 3, respectively. Next, the details of each implementation are discussed.

4.1 Embedding the watermark in SVD1

In both proposed schemes, before embedding the watermark a preprocessing is done on the watermark image. Here the watermark size is 64×64 and the cover size is 1024×1024. The preprocessing makes a redundant watermark image with exactly the size of the cover as it is shown in Fig. 2. Then, one level DWT and consequently SVD is exerted in both cover and watermark images. Afterwards, the singular matrix S_w from the watermark is added to singular matrix S from the cover image using a scaling factor. Finally, reverse SVD and reverse DWT is performed to produce the watermarked image.

Figure 2 shows the process of embedding watermark in SVD1 and SVD2. In this figure, the watermark is assumed to be an image. However, in the general case, it might be any binary sequence. This does not affect the generality of the proposed approach.

The left side of this figure is assigned to explain watermark embedding in SVD1.

The embedding process in SVD1 consists of the following steps:

Step 1: Repeat the watermark redundantly to be matched to the size of the host image.
Step 2: Apply one level DWT to the host and watermark images (if the watermark is not an image, only to the host image).

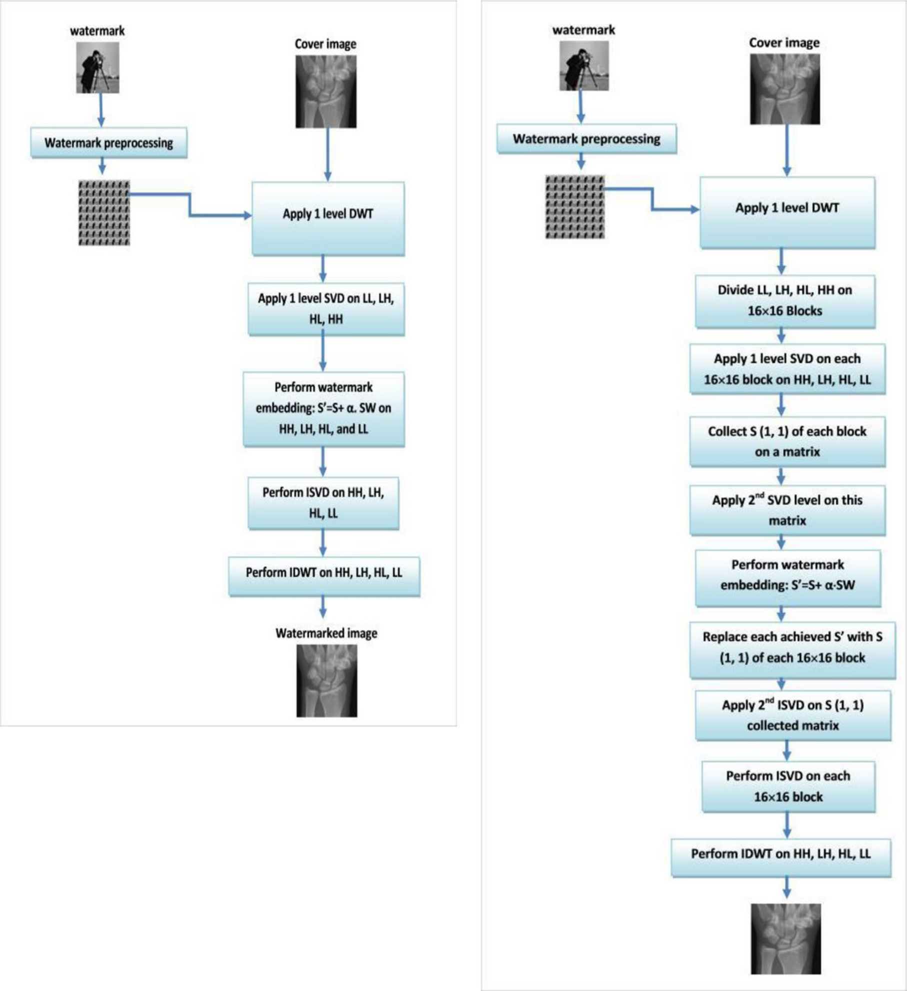

watermark
Cover image
Watermark preprocessing
Apply 1 level DWT
Apply 1 level SVD on LL, LH, HL, HH
Perform watermark embedding: S'=S+ α. SW on HH, LH, HL, and LL
Perform ISVD on HH, LH, HL, LL
Perform IDWT on HH, LH, HL, LL
Watermarked image
watermark
Cover image
Watermark preprocessing
Apply 1 level DWT
Divide LL, LH, HL, HH on 16×16 Blocks
Apply 1 level SVD on each 16×16 block on HH, LH, HL, LL
Collect S (1, 1) of each block on a matrix
Apply 2nd SVD level on this matrix
Perform watermark embedding: S'=S+ α·SW
Replace each achieved S' with S (1, 1) of each 16×16 block
Apply 2nd ISVD on S (1, 1) collected matrix
Perform ISVD on each 16×16 block
Perform IDWT on HH, LH, HL, LL

Fig. 2 Comparison of two schemes in watermark embedding: (Left). DWT + SVD1, (Right). DWT + SVD2

Step 3: Apply one level SVD to each sub-band of the DWT decomposition (for both the host and the watermark images) on the previous step.

Step 4: Perform watermark embedding according to the following formula, where α is a scaling factor, S_H are the singular values of the host image, and W is the watermark (image):

$$S' = S_H + \alpha.W \tag{4}$$

Note that W is a general definition of the watermark which can be everything not necessarily an image. In our implementation we considered singular values of the watermark (S_W) as W in Eq. 4.

Step 5: Perform ISVD with the new singular values of the previous step.

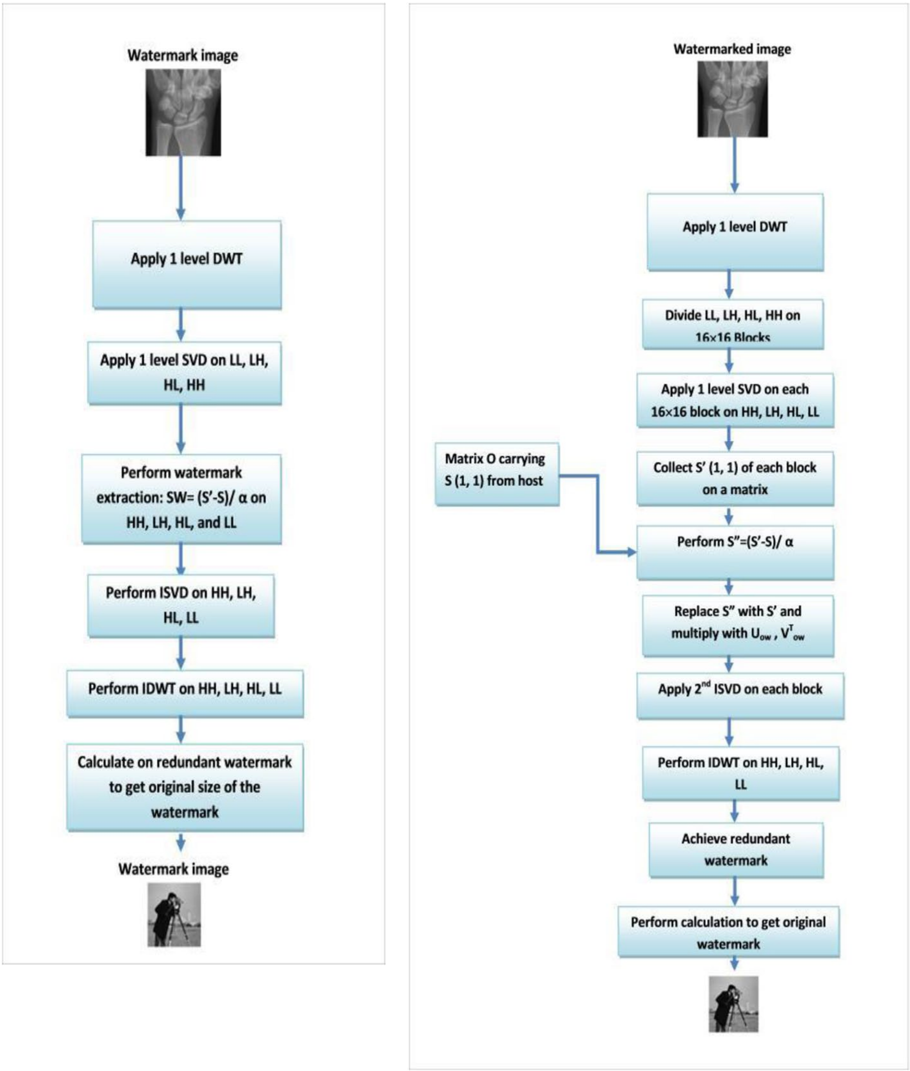

Watermark image
Apply 1 level DWT
Apply 1 level SVD on LL, LH, HL, HH
Perform watermark extraction: SW= (S'-S)/ α on HH, LH, HL, and LL
Perform ISVD on HH, LH, HL, LL
Perform IDWT on HH, LH, HL, LL
Calculate on redundant watermark to get original size of the watermark
Watermark image
Watermarked image
Apply 1 level DWT
Divide LL, LH, HL, HH on 16×16 Blocks
Apply 1 level SVD on each 16×16 block on HH, LH, HL, LL
Matrix O carrying S (1, 1) from host
Collect S' (1, 1) of each block on a matrix
Perform S"=(S'-S)/ α
Replace S" with S' and multiply with U_ow , V^T_ow
Apply 2nd ISVD on each block
Perform IDWT on HH, LH, HL, LL
Achieve redundant watermark
Perform calculation to get original watermark

Fig. 3 Comparison of two schemes in watermark extraction: (Left). DWT + SVD1, (Right). DWT + SVD2

Step 6: Perform IDWT on each sub-band.

Similar to the embedding of the watermark in SVD1, the embedding process for the SVD2 scheme is shown on the right side of the Fig. 2.

4.2 Embedding watermark in SVD2

The embedding process for SVD2 is shown in the right side of Fig. 2. This process consists of the following steps:

Step 1: Repeat the watermark redundantly to be matched to the size of the host image.

Step 2: Apply one level DWT to the host and watermark images.

Step 3: Divide each sub-band of DWT into 16 × 16 non-overlapping blocks.

Step 4: Perform SVD to each block of the pervious step.

Step 5: Collect the highest energetic parts of each block (located on S (1, 1) of each block) on a separate matrix for both the host and watermark images, denoted as the matrix O_H, and the matrix O_W, respectively.

Step 6: Perform a second SVD on the matrices O_H and O_W:

$$\begin{aligned} O_H &= U_{OH} S_{OH} V_{OH}^T, \\ O_W &= U_{OW} S_{OW} V_{OW}^T \end{aligned} \tag{5}$$

Step 7: Perform watermark embedding according to Eq. (6), where α is scaling factor, S_{OH} are the singular values of matrix O_H from the host image while S_{OW} are the singular values of the matrix O_W from the watermark:

$$S\prime_{OH} = S_{OH} + \alpha . S_{OW} \tag{6}$$

Step 8: Apply ISVD on the mentioned matrix:

$$O_H{}' = U_{OH} S'_{OH} V^T{}_{OH} \tag{7}$$

Step 9: Replace the elements S (1, 1) of each 16 × 16 block with the corresponding elements of O_H' for all DWT sub-bands.

Step 10: Apply the ISVD on each block with the new values of singular values stemming from the previous step.

Step 11: Apply IDWT on each sub-band.

Step 12: According to mentioned embedding processes, with identical algorithm in both schemes, SVD2 has 4 steps more than SVD1. We try to understand the effect of these four steps on imperceptibility and robustness of the schemes. These results are analyzed in Section 5.

4.3 False positive and false negative prevention

SVD-based watermarking schemes are generally vulnerable against false positive attack which is defined as the ability of the attackers to inject their fake U and V^T singular vectors to be multiplied with the obtained S singular values in order to elaborate their own watermark from the watermarked image. To neutralize the effect of such attack, we have used the authentication system described in [14] and [11] in which the singular vectors U and V are hashed with the aid of a secret key in the sender side, then, in receiver side before extracting the watermark, the user will send the hash values of his U and V. If the hash values sent by the user are equal to the original hash values of these vectors, the extraction permission is given to user. Otherwise, the user is identified as an unauthorized user and the permission of watermark extraction is not granted. Moreover, by inspiring from authors in [31] a digital signature stemming from hashing of the whole watermark is created to be hidden in the watermarked image such that granting extraction permission to the user is dependent on the combination of the output of this digital signature and the correctness of the hash values of U and V.

4.4 Extracting watermark in SVD1

The process of watermark extraction for both schemes is shown in Fig. 3. The left side of this figure is assigned to the watermark extraction in SVD1 scheme. In order to extract watermark in SVD1 scheme, the subsequent steps need to be performed:

Step 1: Apply DWT to the (presumably) watermarked image W^* which is subjected to attacks.
Step 2: Apply the SVD to each sub-band of DWT stemming from the previous step.
Step 3: Compute S_W^* using the following Equation:

$$S_W^* = \left(S\prime^* - S_H\right)/\alpha \tag{8}$$

Step 4: Multiply S_W^* by U_W and $V^T{}_W$ which are given to the authorized user as secret keys.
Step 5: Apply IDWT to each sub-band.
Step 6: The redundant watermark is achieved now which needs a reverse calculation of step 1 of the embedding process to obtain the watermark with its original size. Note that we did not consider blindness in the algorithms because we just aimed to compare SVD1 and SVD2 under similar circumstances.

The details of the extraction watermark in both SVD1 and SVD2 are shown in Fig. 3.

4.5 Extracting watermark in SVD2

The details of the extraction watermark in SVD2 is shown in the right side of Fig. 3. The extraction for this scheme is described as below:

Step 1: Apply DWT to the (presumably) watermarked image.
Step 2: Divide each DWT sub-band into non overlapping 16×16 blocks.
Step 3: Apply SVD to each block.
Step 4: Collect $S'^*(1, 1)$ of each block on a separate matrix O'^*.
Step 5: Apply SVD to this matrix.
Step 6: Achieve $S^*{}_{OW}$ using the following expression where α is the scaling factor, and S_H is the singular values of the host image (matrix O_H is given to the authorized user):

$$SO_W^* = \left(S\prime_O^* - S_{OH}\right)/\alpha \tag{9}$$

Step 7: Multiply $S^*{}_{OW}$ by U_{OW} and $V^{\mathrm{T}}{}_{OW}$ to achieve matrix $O^*{}_W$, carrying the high energetic parts of the singular values of each block from the watermark image.
Step 8: Replace each element of $O^*{}_W$ matrix by S (1, 1) of each 16×16 corresponding blocks of the matrixes in all DWT sub-bands.
Step 9: Apply ISVD to each block of four DWT sub-bands.
Step 10: Apply IDWT on each sub-band.
Step 11: The redundant watermark is obtained, which needs a reverse calculation following Step 1 in the embedding process to recover the watermark in its original size.

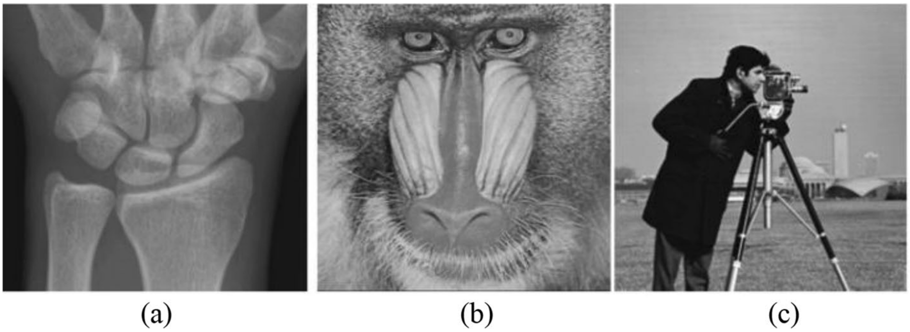


Fig. 4 Sample of tested images: **a**, **b** X-Ray and Baboon as host images **c** cameraman as watermark

5 Experimental results and analysis to compare two schemes

In this section experimental results are presented for two samples of images, one medical image X-Ray of size 1024×1024 and one non-medical image Baboon of size 512×512, as shown in Fig. 4. The original watermark image is Cameraman 64×64. All medical images are real samples of patients taken from "http://radiopedia.org/encyclopedia/cases/". This database has a variety of samples of real medical cases with the different modalities of MRI, CT and X-RAY [41]. Non-medical (typical) samples of images are taken from USC-SIPI image database with the address "http://sipi.usc.edu/database" [47]. Based on the explained embedding and extraction algorithms detailed in Section 4, the experimental results for two schemes are shown and compared in each peer sub-band.

5.1 Test of imperceptibility

In this test, the PSNR of the watermarked images for both SVD1 and SVD2 schemes in two medical and non-medical samples are illustrated. Table 1 shows the comparison of imperceptibility for the medical image X-ray in the proposed SVD1 and SVD2 for each peer DWT sub-band, while Table 2 shows the same comparison for non-medical image Baboon.

As it is shown in these tables, the difference of PSNR in both medical and non-medical images between SVD1 and SVD2 in LL sub-band is more than 10 dB. In addition, there is a good range of imperceptibility for both schemes in this sub-band. In the LH and HL sub-bands, the difference of SVD1 and SVD2 is decreased to 4 dB. Again, in the HH sub-band, this difference is increased to 5 dB in each image type. SVD2 offers superior imperceptibility in terms of PSNR in all DWT sub-bands in comparison to SVD1.

Table 1 Comparison of PSNR in SVD1 and SVD2 for X-RAY

Difference of SVDs	X-RAY			
	LL	HL	LH	HH
SVD1	53.6056	39.1522	40.3121	41.3604
SVD2	65.5593	43.5478	44.697	46.9879

Table 2 Comparison of PSNR in SVD1 and SVD2 for BABOON

Difference of SVDs	BABOON			
	LL	HL	LH	HH
SVD1	61.8291	39.3697	40.388	41.3954
SVD2	77.6624	43.5377	44.84	46.9441

5.2 Test of security

According to Section 4.3, the watermark extraction permission is only given to the authorized parties. As a result, both false positive and false negative effects can be detected and prevented. In this test, we considered a scenario in which attacker tries to extract his own watermark by injecting the fake U and V matrices. As it has been shown in Fig. 5, the extraction permission is denied to be given to the attacker. Figure 5 shows the result of our authentication system to the unauthorized user.

5.3 Test of payload

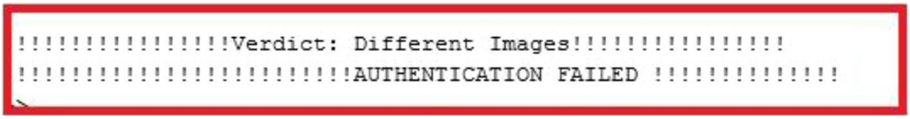
As mentioned before, the original size of the watermark is 64×64 but in the preprocessing phase we increased it redundantly to reach to the size of the cover image. Moreover, an eight bit digital signature is hidden to the host to prevent the false positive effect.

5.4 Test of robustness

In order to show the ability of the watermarked image to withstand against signal processing and geometric attacks, the watermarked image is exposed on the most recognized attacks mentioned in Tables 3 and 4, and the corresponding results are shown for both SVD1 and SVD2 schemes for each of medical and non-medical samples in their peer DWT sub-bands. The difference of robustness between both schemes is proved by showing the visual effect of running 11 types of attacks including 192 images in Tables 3 and 4.

For more clarification, the result of the robustness test in LL sub-band for both X-Ray and Baboon is colored with green. Also, for tangibly showing the variations of robustness between SVD1 and SVD2 all results taken from SVD1 are shown in the brighter colors while results taken from SVD2 are shown in darker colors of green for LL and red for HH sub-bands.

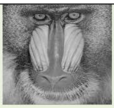
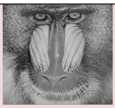
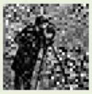
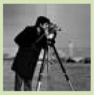
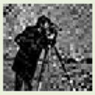
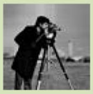
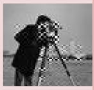
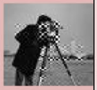
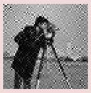
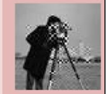
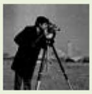
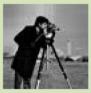
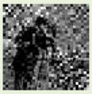
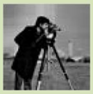
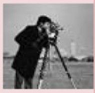
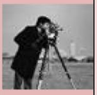
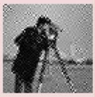
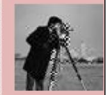
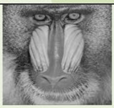
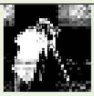
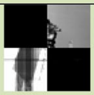
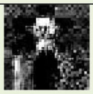
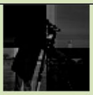
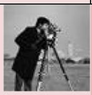
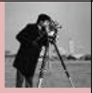
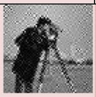
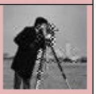
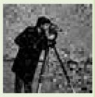
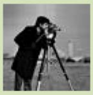
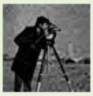
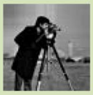
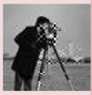
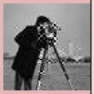
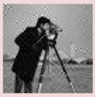
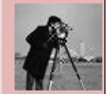
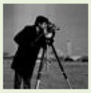
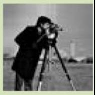
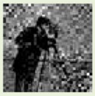
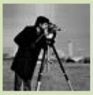
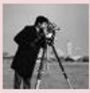
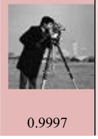
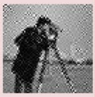
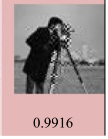
Looking in Table 3, it can be clearly seen that, in the LL sub-band (green district), both schemes show a good range of robustness against noise attacks such as Gaussian, Speckle, Salt and Pepper and, also, filtering attacks such as Average and Median filtering. The



```
!!!!!!!!!!!!!!!!Verdict: Different Images!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!AUTHENTICATION FAILED !!!!!!!!!!!!!!
```

Fig. 5 Result of false positive test in both SVD1 and SVD2

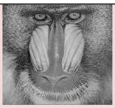
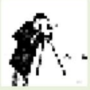
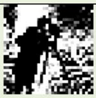
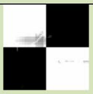
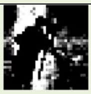
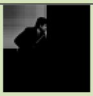
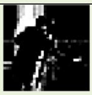
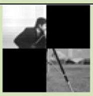
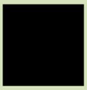
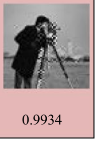
Table 3 Comparison of robustness between SVD1 and SVD2 in LL and HH sub-bands for medical and non-medial image

Attacks & Achieved NC	 **LL Sub-band, Cover: X-ray (1024*1024)**		 **LL Sub-band, Cover: Baboon (512*512)**		 **HH Sub-band, Cover: X-ray (1024*1024)**		 **HH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
No attack								
NC	1	1	1	1	1	1	1	1
GAUSSIAN 0.01								
NC	0.8829	0.9954	0.9375	0.997	0.9548	0.9855	0.9716	0.9929
Average Filtering 3*3								
NC	0.9944	0.9967	0.8548	0.9953	0.9995	0.9999	0.9753	0.9929
Attacks & Achieved NC	 **LL Sub-band, Cover: X-ray (1024*1024)**		 **LL Sub-band, Cover: Baboon (512*512)**		 **HH Sub-band, Cover: X-ray (1024*1024)**		 **HH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
CROP 1/4								
NC	-0.2806	0.6258	0.223	0.6809	0.9993	0.9997	0.9697	0.9915
Salt &Pepper 0.01								
NC	0.982	0.9976	0.9914	0.9956	0.9861	0.9928	0.9965	0.9985
SCALING 512-256-512								
NC	0.9943	0.9969	0.9338	0.9965	0.9993	0.9997	0.9699	0.9916

smoothness of the extracted watermark in SVD2 in comparison to SVD1 is quite clear in the figures for mentioned attacks. On the contrary, except Scaling attack, the watermark image cannot be extracted properly under Gamma Correction, Compression, Rotation, Histogram Equalization and Cropping attacks in both schemes at the LL sub-band.

For Crop ¼, negative sign for NC can be observed for SVD1 in the X-ray image. It happened because the watermark is extracted similar to a negative film in which the dark colors are changed to bright colors and conversely the light colors are changed to the dark colors. That is why the negative amount is achieved for SVD1 in LL sub-band.

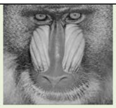
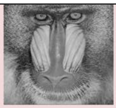
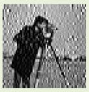
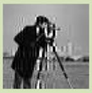
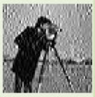
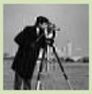
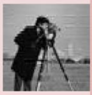
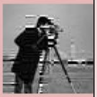
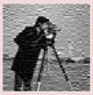
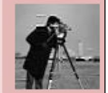
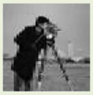
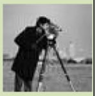
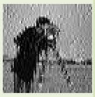
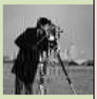
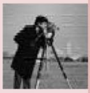
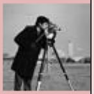
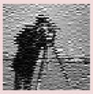
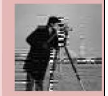
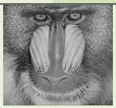
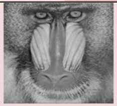
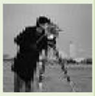
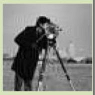
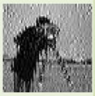
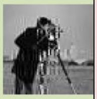
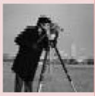
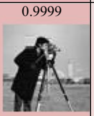
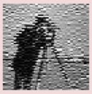
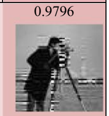
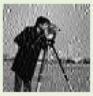
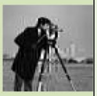
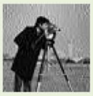
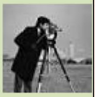
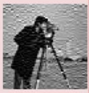
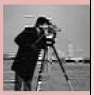
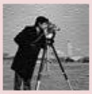
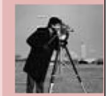
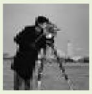
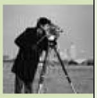
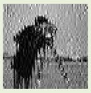
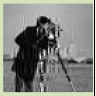
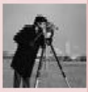
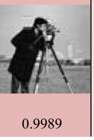
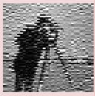
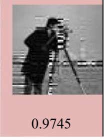
Table 3 (continued)

Attacks & Achieved NC	**LL Sub-band, Cover: X-ray (1024*1024)**		**LL Sub-band, Cover: Baboon (512*512)**		**HH Sub-band, Cover: X-ray (1024*1024)**		 **HH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
Histogram Equalization								
NC	0.8657	0.2521	0.321	0.2038	0.9984	0.9995	0.9761	0.9944
SPECKLE 0.01								
NC	0.9843	0.997	0.9847	0.9968	0.9913	0.9974	0.9965	0.999
MEDIAN 3*3								
NC	0.9927	0.9966	0.9007	0.9849	0.9995	1	0.9854	0.9956
Attacks & Achieved NC	**LL Sub-band, Cover: X-ray (1024*1024)**		**LL Sub-band, Cover: Baboon (512*512)**		**HH Sub-band, Cover: X-ray (1024*1024)**		**HH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
Rotation 50								
NC	0.1054	0.5171	0.3269	0.6087	0.9995	0.9998	0.9929	0.9971
Gamma Correction 0.5								
NC	NAN	NAN	NAN	NAN	0.9992	0.9997	0.9629	0.9886
Compression 50%								
NC	NAN	NAN	NAN	NAN	0.9993	0.9998	0.977	0.9934

In general, correlation coefficients express the strength of the linear relationship among two variables, x and y (here, x indicates as the original watermark and y indicates as extracted watermark). It can be changed between −1 to 1. When this linear correlation coefficient is greater than zero, a positive relationship is designated, while achieving a value that is minus signifies a negative relationship. A zero value indicates there is no relationship between the variables.

A good robustness can be achieved usually with the normalized correlation (NC) more than 0.8000. In LL sub-band (green area), the amount of NC for the mentioned

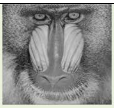
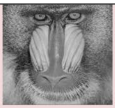
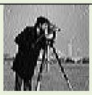
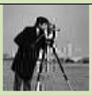
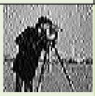
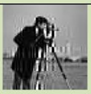
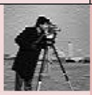
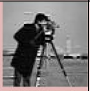
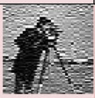
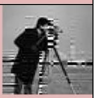
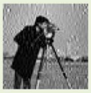
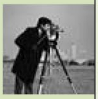
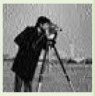
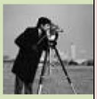
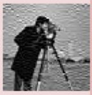
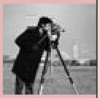
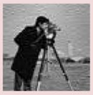
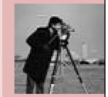
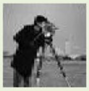
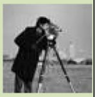
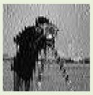
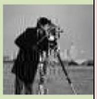
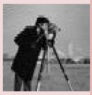
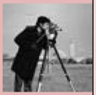
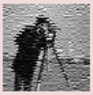
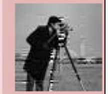
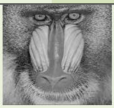
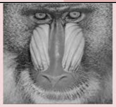
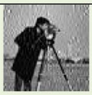
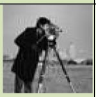
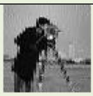
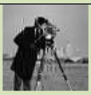
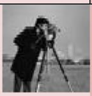
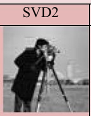
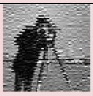
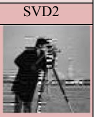
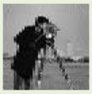
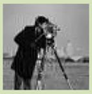
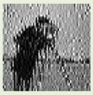
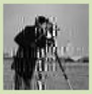
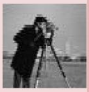
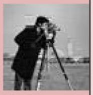
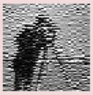
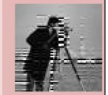
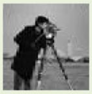
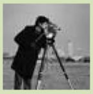
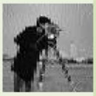
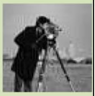
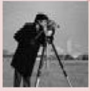
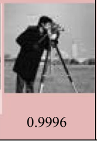
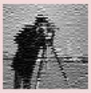
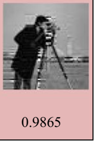
Table 4 Comparison of robustness between SVD1 and SVD2 in HL and LH sub-bands for medical and non-medial image

Attacks & Achieved NC	**HL Sub-band, Cover: X-ray (1024*1024)**		 **HL Sub-band, Cover: Baboon (512*512)**		**LH Sub-band, Cover: X-ray (1024*1024)**		 **LH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
No attack								
NC	1	1	1	1	1	1	1	1
GAUSSIAN 0.01								
NC	0.9685	0.9911	0.9805	0.9967	0.9626	0.9894	0.9884	0.9973
Aerage Filtering 3*3								
Attacks & Achieved NC	**HL Sub-band, Cover: X-ray (1024*1024)**		 **HL Sub-band, Cover: Baboon (512*512)**		**LH Sub-band, Cover: X-ray (1024*1024)**		 **LH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
NC	0.9955	0.9987	0.9754	0.9917	0.9984	0.9999	0.935	0.9796
CROP 1/4								
NC	0.9946	0.9976	0.969	0.9867	0.9973	0.9986	0.9174	0.9764
Salt & Pepper 0.01								
NC	0.9915	0.9961	0.998	0.9995	0.9898	0.9947	0.999	0.9994
SCALING 512-256-512								
NC	0.9954	0.9983	0.9667	0.9865	0.9977	0.9989	0.9121	0.9745

attacks are less than 0.7, and it means that both techniques in LL sub-band are unsuccessful to withstand against Gamma Correction, Compression, Rotation, Histogram Equalization and Cropping attacks while a good performance to resist against the rest of 6 attacks is shown in Table 3.

In the HH sub-band, as it is shown in the red area, the watermarked image is highly robust against all range of examined attacks while SVD2 in darker red areas is more robust than SVD1 in brighter red areas for all of the attack types. The figures can clearly show this claim.

Table 4 (continued)

Attacks & Achieved NC	**HL Sub-band, Cover: X-ray (1024*1024)**		 **HL Sub-band, Cover: Baboon (512*512)**		**LH Sub-band, Cover: X-ray (1024*1024)**		 **LH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
Histogram Equalization								
NC	0.9878	0.9946	0.9574	0.9882	0.9934	0.9948	0.9228	0.9847
SPECKLE 0.01								
NC	0.9949	0.9992	0.9978	0.9996	0.9937	0.9984	0.999	0.9995
MEDIAN 3*3								
NC	0.9955	0.999	0.9831	0.9928	0.9981	0.9996	0.9596	0.9904
Attacks & Achieved NC	**HL Sub-band, Cover: X-ray (1024*1024)**		 **HL Sub-band, Cover: Baboon (512*512)**		**LH Sub-band, Cover: X-ray (1024*1024)**		 **LH Sub-band, Cover: Baboon (512*512)**	
	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2	SVD1	SVD2
Rotation 50								
NC	0.9949	0.9981	0.9905	0.9945	0.9978	0.9991	0.9475	0.981
Gamma Correction 0.5								
NC	0.9922	0.9961	0.9251	0.9731	0.9959	0.9976	0.8498	0.9633
Compression 50%								
NC	0.9972	0.9995	0.9921	0.9974	0.9986	0.9996	0.9635	0.9865

Comparing robustness in LL and HH for both schemes, our observation shows that for both proposed schemes in medical and non-medical images the extracted watermark is robust for all types of attacks while extracted watermarks in SVD2 shows even a better NC which indicates more efficiency for SVD2 scheme in comparison to SVD1. Overall consideration, HH sub-band is offering better robustness and resistance against signal processing and geometric attacks. However, for some attacks, like Gaussian noise or Average filtering, this superiority in robustness will be greater in the LL sub-band only for the SVD2 scheme.

In Table 4, the robustness of the proposed schemes in the HL and LH sub-bands is investigated. Similar to Table 3, the result of robustness in the HL sub-band is shown in green color. All SVD1 results are shown in bright green, whereas SVD2s are shown in dark green for better clarification. The same order of coloring is taken into consideration for the LH sub-band but with red color.

In the HL sub-band (the green area), for both medical and non-medical images, SVD2 shows superior robustness than the SVD1 scheme. As illustrated in the figures, the vertical noise in the extracted watermark in both schemes can be clearly seen but, in SVD2, this vertical noise is decreased such that the extracted watermark is quite smoother than the extracted watermark in SVD1, for the same attack parameters.

The LH sub-band is illustrated in bright and dark red for the SVD1 and SVD2 schemes respectively. The horizontal noise can be seen in extracted watermark in confrontation with attacks like Rotation, Gamma correction, and Compression, where the extracted watermark in SVD2 shows smoother and more robust figures.

In general, for the HL and LH sub-bands in both schemes, the robustness is alternatively different between these two sub-bands. For example, in the X-Ray medical image with size 1024×1024, the LH offers more robustness, whereas in the non-medical image Baboon with size 512×512, the HL sub-band shows better robustness.

In short, the highest robustness in both schemes is obtained to HH and then, according to the size and type of images, HL or LH can be in the second or third places, whereas the LL sub-band, despite offering good robustness, is unable to resist some attacks such as histogram equalization, cropping, compression, rotation and gamma correction, as illustrated in Table 3 for both schemes.

6 Comparison and discussion

In this section, the proposed SVD1 and SVD2 schemes are compared with several recent proposed counterparts. The difference of imperceptibility between the proposed schemes and these schemes for Baboon image is shown in Table 5. It is observed that the proposed SVD2 scheme is more imperceptible than [6], [51] and [49], [2] but Aree et al.'s scheme [34] has a larger PSNR compared to the proposed scheme. Besides, the proposed SVD1 scheme has better imperceptibility than [6] and [49].

Table 6 shows the comparison of robustness according to Normalized Correlation coefficient (NC) between the SVD1 and SVD2 schemes. Looking at this table, it can be clearly seen that the proposed SVD2 scheme is more robust for 6 out of 11 attacks in comparison to the other schemes. Ali et al.'s scheme [6] has better robustness only in confronting two attacks (Histogram equalization and Gamma correction), and Wang and Zhao's scheme [49] can withstand against Median filtering, Compression and Gaussian noise. Ahmadi et al.'s scheme shows the best performance against Cropping and Gamma Correction. The proposed SVD2 scheme shows an excellent robustness compared to the other schemes for the remaining seven types of attacks.

The watermarking scheme proposed by Zeng et al. [51] offers better robustness in attacks like scaling and compression, but less robustness in the remaining of the other attacks in comparison to our propose SVD2 scheme.

Furthermore, Aree et al.'s scheme [34] shows the NC of 0.955 even in the situation of "no attack" while it is only robust against Salt and Pepper attack in comparison to both proposed schemes.

Table 5 Comparison of imperceptibility according to peak signal to noise (PSNR) amongst SVD1, SVD2 and other related works for Baboon image

Scheme	Ali [6] SVD + DWT + ABC	Aree [34] DWT + SVD+ zigzag embedding	Wang [49] DWT3 + SVD	Zeng [51] NSCT+DWT + SVD + HVS	Ahmadi [2] DWT + SVD + PSO	Our DWT + SVD1	Our DWT + SVD2
PSNR	40.0256	47.636	40.17	46.8550	43.2199	41.3954	**46.9441**

Bold entries indicate the best results

Table 6 Comparison of robustness amongst SVD1, SVD2 and other related works

Schemes	Ali 2015 [6]	Aree 2020 [34]	Wang 2020 [49]	Ahmadi 2021 [2]	Zeng 2022 [51]	Proposed	Proposed
Watermark size	(32*32)	(128*128)	(128*128)	(64*64)	(32*32)	DWT + SVD1 (cover size)	DWT + SVD2 (cover size)
Attacks							
No attack	1	0.955	1	1	1	1	**1**
Average filtering (3*3)	NA	NA	NA	NA	NA	0.9753	**0.9929**
Median filtering (3*3)	0.9076	0.4726	0.9969	0.9880	0.9861	0.9854	0.9956
Gaussian noise (0.01)	0.9830	NA	0.9991	0.9886	0.9774	0.9716	**0.9929**
Salt & pepper 0.01	0.8104	0.909	0.9933	0.9886	0.9605	0.9965	**0.9985**
Speckle 0.01	NA	NA	0.9982	0.9968	0.9894	0.9965	**0.9990**
Gamma correction 0.5	**0.9973**	0.6589	0.7634	**1**	NA	0.9629	0.9886
Scaling (512-128-512)	0.9134	NA	0.9909	0.9778	**1**	0.9699	0.9916
Crop 1/4	0.8490	NA	NA	**1**	0.5131	0.9697	0.9915
Rotation 50	0.9988	NA	0.3676	0.9949	0.8150	0.9929	**0.9971**
Histogram equalization	0.9982	NA	0.7598	0.9741	NA	0.9761	**0.9944**
Compression 50%	0.9574	NA	**0.9994**	0.8038	1	0.977	0.9934

Bold entries indicate the best results

In the heading of Table 6, the watermark size of each scheme is shown. In both proposed schemes, the size of the watermark images are equal to the size of cover or host images, which is at least 512×512, while none of the other schemes has offered such property.

Finally, to obtain a better balance between imperceptibility and robustness, other compared schemes in Table 6 use some techniques like Zigzag embedding, Non Sub sampled Contourlet Transformation, Particle Swarm Optimization or Artificial Bee Colony, which effects on cost and computational complexity. On the other hand, the proposed schemes are simple and easy to implement. In particular, the proposed SVD2 scheme is considerably more efficient with only a few extra steps for implementation.

7 Conclusion and future work

A subtle design and implementation of algorithms can decrease the computational burden and cost, while at the same time; increase the performance (imperceptibility and robustness) of watermarking algorithms. Of course, depending on the application, the requirements can be varied between three specifications of robustness, capacity and imperceptibility. As we have shown in this paper, only taking a few extra steps the implemented schemes can be more efficient than those that use some subsidiary algorithms like Artificial Bee Colony or zigzag embedding to achieve optimum values for imperceptibility and robustness. In future work, we intend to implement other hybrid schemes with SVD2 and DCT or DFT.

Acknowledgements The authors acknowledge the funding obtained by the Detection of fake newS on SocIal MedIa pLAtfoRms project from the EIG CONCERT-Japan with grant PCI2020-120689-2 (Government of Spain), and to the RTI2018-095094-B-C22 "CONSENT" and PID2021-125962OB-C31 "SECURING" projects granted by the Spanish Ministry of Science and Innovation.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Declarations

Conflict of interest The authors declare that they have no conflicts of interest.

References

1. Abdallah HA et al (2011) Blind wavelet-based image watermarking. International Journal of Signal Processing, Image Processing and Pattern Recognition 4(1):15–28
2. Ahmadi SBB, Zhang G, Rabbani M, Boukela L, Jelodar H (2021) An intelligent and blind dual color image watermarking for authentication and copyright protection. Appl Intell 51:1701–1732
3. Akhaee MA, Marvasti F (2013) A survey on digital data hiding schemes: principals, algorithms, and applications. ISC Int J Inf Secur 5:5

4. Ali M, Ahn CW (2014) An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. Signal Process 94:545–556
5. Ali M, Ahn CW, Siarry P (2014) Differential evolution algorithm for the selection of optimal scaling factors in image watermarking. Eng Appl Artif Intell 31:15–26
6. Ali M, Ahn CW, Pant M, Siarry P (2015) An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. Inf Sci 301:44–60
7. Ali M, Wook Ahn C, Pant M, Kumar S, Singh MK, Saini D (2020) An optimized digital watermarking scheme based on invariant DC coefficients in spatial domain. Electronics 9:1428
8. Anand A, Singh AK (2020) RDWT-SVD-firefly based dual watermarking technique for medical images (workshop paper). In: 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM), pp 366-372
9. Araghi TK (2019) Digital image watermarking and performance analysis of histogram modification based methods. In: Arai K, Kapoor S, Bhatia R (eds) Intelligent computing. SAI 2018. Advances in intelligent systems and computing, vol 858. Springer, Cham. https://doi.org/10.1007/978-3-030-01174-1_49
10. Araghi TK, Manaf ABA (2017) Evaluation of Digital Image Watermarking Techniques. In: International Conference of Reliable Information and Communication Technology, pp 361-368
11. Araghi TK, Manaf AA (2019) An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. Futur Gener Comput Syst 101:1223–1246
12. Araghi TK, Manaf ABA, Araghi MZSK (2016) Taxonomy and performance evaluation of feature based extraction techniques in digital image watermarking. Int J Image Process Tech– IJIPT 3:20–23
13. Araghi TK, Manaf ABA, Zamani M, Araghi SK (2016) A survey on digital image watermarking techniques in spatial and transform domains. Int J Adv Image Process Tech– IJIPT 3:6–10
14. Araghi TK, Manaf AA, Araghi SK (2018) A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. Expert Syst Appl 112:208–228
15. Araghi TK, Alarood AA, Araghi SK (2021) Analysis and evaluation of template based methods against geometric attacks: a survey. In: Saeed F, Mohammed F, Al-Nahari A (eds) Innovative systems for intelligent health informatics. IRICT 2020. Lecture Notes on Data Engineering and Communications Technologies, vol 72. Springer, Cham. https://doi.org/10.1007/978-3-030-70713-2_73
16. Arora SM, Kadian P (2022) Enhanced image security through hybrid approach: protect your copyright over digital images. Wireless Communication Security, pp 35–57
17. Bansal M, Mishra A, Sharma A (2020) Optimized DWT SVD Based Image Watermarking Scheme Using Particle Swarm Optimization. In: International conference on computational science and its applications, pp 862–877
18. Bhuyan HK, Chakraborty C (2022) Explainable machine learning for data extraction across computational social system. In IEEE Transactions on Computational Social Systems. https://doi.org/10.1109/TCSS.2022.3164993
19. Chakraborty C, Mishra K, Majhi SK, Bhuyan HK (2022) Intelligent latency-aware tasks prioritization and offloading strategy in distributed fog-cloud of things. IEEE Trans Industr Inform 19:2099–2106
20. Chandrakar N, Bagga J (2013) Performance comparison of digital image watermarking techniques: a survey. Int J Comput Appl Technol Res 2:126–130
21. Chaturvedi N, Basha S (2012) Comparison of digital image watermarking methods DWT & DWT-DCT on the basis of PSNR. Image 2:1
22. Danyali H, Makhloghi M, Tab FA (2012) Robust blind dwt based digital image watermarking using singular value decomposition. Int J Innov Comput Inf Control 8:4691–4703
23. Dhawan S et al (2022) An efficient steganography technique based on S2OA & DESAE model. Multimed Tools Appl 1–29
24. Dittmann J, Megias D, Lang A, Herrera-Joancomarti J (2006) Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity. In: Transactions on data hiding and multimedia security I, ed. Springer, pp 1–40
25. Guo X, Zhuang T-g (2009) A region-based lossless watermarking scheme for enhancing security of medical data. J Digit Imaging 22:53–64
26. Gupta M, Parmar G, Gupta R, Saraswat M (2015) Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony. Int J Comput Intell Syst 8:364–380
27. Hussein E, Belal MA (2012) Digital watermarking techniques, applications and attacks applied to digital media: a survey. Threshold 5:6
28. Khanam T, Dhar PK, Kowsar S, Kim J-M (2020) SVD-based image watermarking using the fast Walsh-Hadamard transform, key mapping, and coefficient ordering for ownership protection. Symmetry 12:52

29. Koohpayeh Araghi T, Abd Manaf A, Alarood A, Zainol AB (2018) Host feasibility investigation to improve robustness in hybrid DWT+SVD based image watermarking schemes. Adv Multimed 2018:1609378
30. Mahajan PH, Bhalerao PB (2014) A review of digital watermarking strategies. Int J Adv Res Comput Sci Manag Stud 7
31. Makbol NM, Khoo BE (2014) A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. Digit Signal Process 33:134–147
32. Makbol NM, Khoo BE, Rassem TH, Loukhaoukha K (2017) A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Inf Sci 417:381–400
33. Makbol NM, Khoo BE, Rassem TH (2018) Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. Multimed Tools Appl 77:26845–26879
34. Mohammed AA, Salih DA, Saeed AM, Kheder MQ (2020) An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique. Multimed Tools Appl 79:32095–32118
35. Moon SK (2022) Authentication and security aspect of information privacy using anti-forensic audio–video embedding technique. In: Inventive systems and control: proceedings of ICISC 2022, ed. Springer, pp 157-171
36. Moon SK (2022) Application of forensic audio-video steganography technique to improve security, robustness, and authentication of secret data, Cham, pp 11–25
37. Nikolaidis A (2012) Local distortion resistant image watermarking relying on salient feature extraction. EURASIP J Adv Signal Process 2012:1–17
38. Nyeem H, Boles W, Boyd C (2012) On the robustness and security of digital image watermarking. In: Informatics, electronics & vision (ICIEV), 2012 international conference on, pp 1136–1141
39. Pan Z, Hu S, Ma X, Wang L (2015) A new lossless data hiding method based on joint neighboring coding. J Vis Commun Image Represent 26:14–23
40. Qian Z, Zhang X, Ren Y (2015) JPEG encryption for image rescaling in the encrypted domain. J Vis Commun Image Represent 26:9–13
41. Radiopaedia.org [Online]. Available: https://radiopaedia.org/cases?lang=us. Accessed 12 May 2023
42. Rawat N, Manchanda R (2014) Review of methodologies and techniques for digital watermarking. Int J Emerg Technol Adv Eng 4(4):237–240
43. Shojanazeri H, Adnan WAW, Ahmad SMS (2013) Video watermarking techniques for copyright protection and content authentication. Int J Comput Inf Syst Ind Manag Appl 5:652–660
44. Singh AK, Dave M, Mohan A (2014) Wavelet based image watermarking: futuristic concepts in information security. Proc Natl Acad Sci India Sect A Phys Sci 84:345–359
45. Tao H, Chongmin L, Zain JM, Abdalla AN (2014) Robust image watermarking theories and techniques: a review. J Appl Res Technol 12:122–138
46. Thapa M, Sood SK, Sharma AM (2011) Digital image watermarking technique based on diferent attacks. Int J Adv Comput Sci Appl 2(4):14–19. https://doi.org/10.14569/IJACSA.2011.020402
47. The USC-SIPI Image Database [Online]. Available: https://sipi.usc.edu/database/. Accessed 12 May 2023
48. Wan W et al (2022) A comprehensive survey on robust image watermarking. Neurocomputing. https://doi.org/10.1016/j.neucom.2022.02.083
49. Wang B, Zhao P (2020) An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain. Mathematics 8:691
50. Yuan X-C, Pun C-M (2014) Feature extraction and local Zernike moments based geometric invariant watermarking. Multimed Tools Appl 72:777–799
51. Zeng F, Bai H, Xiao K (2022) Blind watermarking algorithm combining NSCT, DWT, SVD, and HVS. Secur Priv 5(4):e223

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.